Bibliografía y Fuentes
Charla RF: Hackemate

Alan Levy / Matias Perez
@mtg_security
Marzo de 2018

Ataques

Jamming:
Jammin WiFi with GNURadio
https://advancedpersistentjest.com/2017/04/17/signal-disruption-via-gnuradio/

Rolling Codes
RollJam en GNURadio:
http://spencerwhyte.blogspot.com.ar/2014/03/delay-attack-jam-intercept-and-replay.html

The Five Finger Code Finder (vehículos Ford)
https://hackaday.io/project/27445-five-finger-code-finder

Ataque teclado inalambrico
https://samy.pl/keysweeper/#key
http://travisgoodspeed.blogspot.com.ar/2011/02/promiscuity-is-nrf24l01s-duty.html

Ataque Alarmas
https://www.youtube.com/watch?v=68M6IVNxjfg

Detector de microfonos espias usando SDR
https://github.com/eldraco/Salamandra

Charlas, Presentaciones y otras:

Hacking The IoT (Internet of Things) - PenTesting RF Operated Devices
https://www.owasp.org/images/2/29/AppSecIL2016_HackingTheIoT-PenTestingRFDevices_ErezMetula.pdf

DEF CON 25 - Matt Knight - Radio Exploitation 101

https://www.youtube.com/watch?v=HTVPmF8u7Yg

Decodificando señal de garaje con audacity
https://www.youtube.com/watch?v=IAa2EXsvYHA

Ver la pantalla de un monitor con SDR (Tempest)
https://github.com/martinmarinov/TempestSDR
https://www.youtube.com/watch?v=8HV70b-DpE0&list=PLjlbvd0_rCDGZJ-WStdmcHxI8W9cb885k
https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/

Explicación de bloques GNU Radio en Replay Atack
https://www.youtube.com/watch?v=RnAgqGR-D-8

Blog de un speaker de la DefCon que dió charla de RF
https://calebmadrigal.com

Decodificando señales con Inspectrum
https://www.youtube.com/watch?v=tGff31uGXQU

433MHz ASK signal analysis
https://bytebucket.org/rootbsd/433mhz-ask-signal-analysis/raw/5f4937e4efb2198abcc375b8aefee41421941fca/pdf/433MHz_ASK_sginal_analysis-Wireless_door_bell_adventure-1.0.pdf

Estudiando comunicaciones por radio con GNURadio y SDR
https://foo-manroot.github.io/post/es/gnuradio/sdr/2017/11/18/gnuradio-ook.html

Suplantando un mando a distancia usando SDR y GNURadio

https://foo-manroot.github.io/post/es/gnuradio/sdr/2018/01/15/gnuradio-ook-transmit.html

JUST A PAIR OF THESE $11 RADIO GADGETS CAN STEAL A CAR

https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/

Arduino

Copiar Señal y replicarla en un Arduino
http://www.instructables.com/id/Decoding-and-sending-433MHz-RF-codes-with-Arduino-/

How to copy a 433MHz signal with an Arduino board

https://www.youtube.com/watch?v=LbCDpbWrdIQ

Arduino, clonado de frecuencias:
https://www.youtube.com/watch?v=LbCDpbWrdIQ

GNU Radio Companion and Practical Sigint

http://blog.kismetwireless.net/2013/08/hackrf-pt-2-gnuradio-companion-and.html

GNU Radio

Decodificando señales

https://blog.compass-security.com/2016/09/software-defied-radio-sdr-and-decoding-on-off-keying-ook/
https://github.com/CBrunsch/BinViz

On-Off Keying (ASK) with SDR

https://zeta-two.com/radio/2015/06/23/ook-ask-sdr.html

Reverse engineering static key remotes with gnuradio and rfcat

https://leonjza.github.io/blog/2016/10/02/reverse-engineering-static-key-remotes-with-gnuradio-and-rfcat/

Ejemplos con HackRF

https://github.com/scateu/HackRF_Examples

GNU Radio Live

https://www.gnuradio.org/blog/using-gnu-radio-live-sdr-environment/

Tools

RFCat Tools

https://github.com/AndrewMohawk/RfCatHelpers

OOK Tools

https://leonjza.github.io/blog/2016/10/08/ooktools-on-off-keying-tools-for-your-sdr/

Decoder de OOK

https://github.com/leonjza/ooktools
https://github.com/jimstudt/ook-decoder

Compendio de tools y hardware:

https://github.com/cn0xroot/RFSec-ToolKit

Envío de señales OOK con Hackrf

https://github.com/Lefinnois/hackrf_ook

Más tools sobre diferencias entre tipos de señales
https://github.com/calebmadrigal/radio-hacking-scripts

Aviones en tiempo real en el navegador con JS
https://github.com/watson/airplanejs

RF, terminología, etc

https://www.youtube.com/watch?v=FVmTooGICNc

SDR

https://greatscottgadgets.com/sdr
https://www.rtl-sdr.com

Y por último mucho, pero mucho: https://www.google.com